[19]中华人民共和国国家知识产权局

[51]Int. Cl[7]
G06F 12/14
G06F 12/16

[12]发明专利申请公开说明书

[21]申请号 00136751.X

[43]公开日 2002年7月31日

[11]公开号 CN 1361481A

[22]申请日 2000.12.28 [21]申请号 00136751.X

[71]申请人 中国科学院计算技术研究所
地址 100080 北京市海淀区中关村科学院南路6号
[72]发明人 庄 超 李国杰 谭建龙

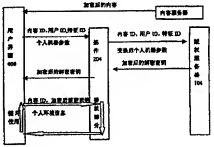
[74]专利代理机构 中科专利商标代理有限责任公司
代理人 朱海波

权利要求书2页 说明书10页 附图页数11页

[54]发明名称 基于网络浏览器插件的版权保护方法

[57]摘要

一种数字版权保护方法，通过对于数字媒体内容进行加密，并在网络环境下借助包含解密密钥的许可证对于数字出版物内容的打印、编辑和播放等使用权利进行控制，其特征在于，包括如下几个步骤：内容服务器形成内容容器的步骤；客户认证内容容器的步骤；许可证的生成与传送步骤；客户在可信环境之中使用内容步骤。



ISSN1008-4274

权 利 要 求 书

1．一种数字版权保护方法，通过对于数字媒体内容进行加密，并在网络环境下借助包含解密密钥的许可证对于数字出版物内容的打印、编辑和播放等使用权利进行控制，其特征在于，包括如下几个步骤：

内容服务器形成内容容器的步骤；

客户认证内容容器的步骤；

许可证的生成与传送步骤；

客户在可信环境之中使用内容步骤。

2．根据权利要求 1 所述的数字版权保护方法，其特征在于，在内容服务器形成内容容器的步骤中将要保护的数字媒体内容通过加密形成内容容器，使得内容容器的内容只能是通过得到密钥之后解密播放，同时对于内容容器添加消息文摘，通过消息文摘判断内容的完整性。

3．根据权利要求 1 所述的数字版权保护方法，其特征在于，在客户认证内容容器的步骤中在客户得到加密的内容容器之后，验证内容容器的完整性，如果验证不成功，则不能打开加密的内容容器。

4．根据权利要求 1 所述的数字版权保护方法，其特征在于，在许可证的生成与传送过程中解密特定的内容容器，同时能够按照客户方的版权的权利请求执行，需要从版权服务器取得对于特定的内容容器所需要的许可证，许可证通过特定步骤生成，然后将许可证从版权服务器传送到客户方。

5．根据权利要求 1 所述的数字版权保护方法，其特征在于，在客户在可信环境之中使用内容步骤中使得用户对于需要版权保护的内容在客户方的可信环境之中执行处理，其中内容和内容的密钥不会被泄露，而内容的显示、打印和编辑只是根据权利请求而执行。

6．根据权利要求 5 所述的数字版权保护方法，其特征在于，通过在网络浏览器的插件之中实现在客户在可信环境之中使用内容步骤。

7．根据权利要求 6 所述的数字版权保护方法，其特征在于，插件是

从远程的版权服务器上取得解密密钥，取得的传送过程是通过安全协议安全传送，传送协议的执行也是通过插件完成。

8．根据权利要求 6 所述的数字版权保护方法，其特征在于，插件作为隔离浏览器上执行网络内容和操作系统文件系统之中内容的屏蔽机制，使得浏览器上的内容可以不被操作系统上的函数调用操作，由于其分离的隔离作用，保护了浏览器界面上的内容。

9．根据权利要求 3 所述的数字版权保护方法，其特征在于，插件利用数字签名检查得到的版权内容的完整性。

说　　明　　书

基于网络浏览器插件的版权保护方法

本发明涉及一种版权保护方法，特别涉及一种在网络上保护作品版权的保护方法。

现在内容提供者拒绝把有价值的媒体内容（数字图书、数字音乐等）在 Internet 上发行，其中的主要原因是对于数字媒体的修改、复制和重新分发非常容易。为了能够将数字媒体商业化，从内容提供者的角度上看，主要是要有技术手段保护作者和出版者的版权，使得一方面作者和出版者的利益能够得到保证，另一方面是确保内容消费者接受的信息内容的完整性和真实性，这是通过数字版权技术解决的问题。随着电子商务的发展，电子付费系统已经取得了很大的进展，而版权保护技术还是一个亟待解决的问题。现有的版权保护技术分为两大类，一是基于水印的标记法，它是一种借助技术手段取得法律证据，最终借助法律手段保护版权的方法。一些攻击手段如 IBM 攻击可能使水印失效。另一种是加密的方法，加密法主要是通过技术手段限制非授权用户的使用和保证授权用户的正常支持使用。现在已经有 CITED、COPICAT、ACCOPI、TALISMAN、IMPRIMATUR 等研究项目对于网络内容的版权开展了研究。若干公司提供了相关的技术产品，主要有 IBM 公司的 Cryptolope 技术，InterTrust 公司的 DigiBox 技术，Breaker 技术公司的 SoftSeal 等等在 Internet 上的内容的版权保护的实质是对于内容的远程的持久的访问控制。本文就版权保护的技术路线主要是通过加密、认证等一系列措施实现对于 Internet 上内容的持久的访问控制。

本发明的一个目的是提供一种利用插件实现版权保护的方法。

本发明的另一个目的是提供一种通过加密、认证等一系列措施实现对于 Internet 上内容的持久的访问控制的方法。

本发明的另一个目的是提供一种用于版权保护的 SKCC(Secure

Kernel-based Content-Control Dual Authenticated Model 基于安全内核的内容控制双重认证协议模型)模型。

本发明的另一个目的是提供一种满足互联网的基本安全需求的版权保护方法。

本发明提供一种数字版权保护方法，通过对于数字媒体内容进行加密，并在网络环境下借助包含解密密钥的许可证对于数字出版物内容的打印、编辑和播放等使用权利进行控制，其中包括如下几个步骤：内容服务器形成内容容器的步骤；客户认证内容容器的步骤；许可证的生成与传送步骤；客户在可信环境之中使用内容步骤。

下面参照附图具体描述本发明：

图 1 为系统流程图： 描述网络上内容的处理流程。

图 2 为插件层次图： 描述插件的层次上的隔离作用。

图 3A-3C 为内容容器格式和许可证文件格式。

图 4 为插件处理流程图：描述插件的处理流程。

图 5 为用户界面图 1：用户的输入界面。

图 6 为用户界面图 2 ：系统控制显示输出的界面。

图 7 为为基于安全内核的内容-控制双重认证协议 SKCC 的模型。

图 8A 至图 8D 为本发明的 SKCC 协议的流程图。

在图 1 中， 数字作品内容 100 打包形成安全内容容器 101，安全内容容器 101 通过 Web（102）的 http （或者 nntp，ftp, smtp）协议传送给用户,用户进行数字作品内容 100 的完整性认证, 用户向版权服务器 104 付费购买许可的权限。 版权服务器 104 提供权限的许可证在浏览器插件 204 中数字作品内容容器 101 按照许可证上的权限执行。

在图 2 中，安全内容的保护分为两个层次，一是直接对于解密的内容的保护，防止内容在 I/O 设备上的泄露；一是对于加密内容的密钥的保护，防止密钥在传送通道和隐秘通道上的泄露。前面我们讨论了两个主要方面的威胁：垂直威胁和水平威胁。对于水平威胁的安全性主要是通过许可证服务器、加密内容和客户方的安全认证协议完成，这里包括密钥在传送通道上安全性的问题。我们通过 Netscape Navigator 202 和插件 Plugin 204 构造的安全可信环境主要是对付垂直方向的威胁，通过它

隔离内容。在我们的客户方的机器系统硬件 200 之上是系统操作系统 201，操作系统 201 之上浏览器系统 202。它们三者构成 Internet 虚拟机 IVM 203。Pl 系统边界就是人与机器的接口的部分。这样我们将从外部硬拷屏和非法获得用户的帐号归为系统边界之外的安全问题。当然对于媒体内容加上水印也可防止硬拷屏幕，但在这里不是我们的考虑范围。防止 I/O 的内容泄露包括硬盘（Cache），显示器（打印、显示和编辑控制）等安全周界的接口。

图 3A 为内容容器文件逻辑形式。图 3B 为文件物理形式。图 3C 为许可证文件逻辑形式。图中表示内容容器文件由用 DES 加密的文件，用机器参数加密的 DES 的密钥以及校验部分三部分构成。许可证文件如图上的五个部分组成。文件的格式描述如图。

在图 4 中，软件基本结构包括两个部分，一是客户通过用户界面 400 对本地插件程序 204 的访问，它确保只有插件程序 204 才能访问加密内容。另一个是版权服务器 104 和插件程序 204 的通讯协议，这个协议使版权服务器传送许可证可以控制用户的操作方式。

图 5 为设计的系统用户界面。在浏览器之中用户在左边用户和口令对话框之中输入口令和用户名，同时选择右边打印，编辑等的申请权利。

图 6 为设计的系统用户界面。在浏览器显示受限制的权利要求的文本文件。

在图 7 中，IVM(Internet Virtual Machine)是由客户方的机器及其操作系统和 Web 浏览器系统共同组成，安全内核是 Web 浏览器的插件系统实现隔离的功能，内容播放程序也是浏览器插件系统的一部分，用户从内容服务器得到加密的内容容器之后，在用户空间之中，选择相关的权利要求通过 Web 传送回版权服务器，版权服务器根据权利要求生成许可证传回用户，用户在内容播放程序之中解密播放加密的内容。

下面介绍本发明所依据的超级分发的 SKCC 模型。

超级分发的 SKCC 模型

1. 超级分发的概念

超级分发（SuperDistribution）的概念是 Ryochi Mori 于 1987 年首先

提出的。他为基于加密的版权保护提供了最原始的模型，Mori 描述了在网络上软件和数字内容的超级分发必须满足的四种属性：

- 数字作品能够在网络上自由的发布，用户使用数字作品需要付费，用户不拥有数字作品的版权；
- 网络上数字作品的提供者可以对于数字作品的使用者（用户）设置条件和费用要求；
- 数字作品需要在合适的平台上运行，但是用户必须满足数字作品的提供者设置的条件和支付相应的费用
- 数字作品可能需要网络的服务器系统加工处理，使得用户需要特殊的设备和特殊的软件平台）才能访问和阅读。

2. 安全性的要求

针对超级分发的概念，我们设计了一种基于加密的电子商务的协议模型 SKCC 模型实现数字内容的安全分发和版权保护。这里我们考虑的安全性的要求主要是有以下的五个方面：

- 安全性不低于非数字出版物：对于纸质出版物可用照相机、复印机和扫描仪等进行复制，但是会增加一定的成本。在开放的网络环境下应该限制数字作品的非法散布和盗版使用。对于纸质出版物的有限拷贝（Hard Copy）在数字化环境中变为无限拷贝。
- 身份认证和内容认证：用户应该能够对于购买的数字作品进行认证，防止中途的窜改。同时服务器应该对于购买用户的身份进行认证，防止假冒的用户的购买。
- 不同的安全级别：电子出版系统应在保证质量和尽可能低成本的条件下，对于不同的数字作品进行不同的安全级别的保护。
- 反设计工程无利可图：使得解密一个文件足够困难同时成本很高，而且即使解开一个文件也不影响其他文件的安全性。
- 隐私性：确保用户购买的数字作品的种类和数量信息不被泄露。

这里 Internet 版权保护的系统必须满足的基本的安全需求是：

- 内容的完整性：内容没有被病毒和其他传输中的因素破坏；
- 特洛伊木马：内容使用者使用木马术窃取密码；
- 安全传输：内容在传送之中没有被破坏；
- 非授权的泄露：违反授权的要求读取和使用内容；
- 复制：内容被非法复制；
- 条件的访问控制：内容没有按照许可证要求的方式使用操作。

3. SKCC 协议模型

SKCC 协议的基本体系结构包括两个部分，一是内容服务器与客户程序之间的安全协议，这个协议主要是确保加密内容（内容容器）的完整的传送到客户处，另一个是版权服务器与客户程序之间的协议，这个协议是将解开内容容器的许可证（版权）安全传送给客户程序。图 1 为内容-控制双重认证协议的体系结构。客户程序需要在可信的计算环境之中，而且客户程序本身需要是一个基于安全内核的计算。

在这个 SKCC 模型中，我们可以将内容和控制分别放在不同的服务器系统上，对于内容的协议主要是确保内容的完整性（免于被窜改）。而对于版权服务器是在内容被驱动之后（付费之后），为了安全通信，在通信过程中需要建立会话密钥，确保加密安全通信。然后将标识信息的凭据对象送给版权服务器，这是因为凭据对象中可以确保机器和内容的唯一性。版权服务器提供相应的许可证。根据许可证的许可，内容可以在可信任的环境下基于安全内核的执行控制方式实现多媒体内容的安全播放。值得注意的是有这样的情况，对于客户方的安全内核取得许可证之后，还可以转发许可证，这种情况也需要安全内核的隔离作用确保许可证内容免于泄露。

4. 协议描述

下面采用代码方式描述本发明的协议。

基本符号描述：

nonce　　生成的随机量（Nonce）

Co	生成的凭据对象.
H（m）	单向的 Hash 函数
MAC（m）	由私钥 K 生成的消息认证
A→B：m	A 传消息 m 给 B
Kc ：	为内容的对称私钥，加密内容
igoods：	为信息商品
Tag：	客户的标记的信息
A：	客户
B：	许可证服务器
C：	内容服务器
Kb, Kb’	B 的公钥和私钥
Ka， Ka’	A 的公钥和私钥
$Sig_k(X)$	X 的数字签名

基本符号描述：

nonce	生成的随机量（Nonce）
H（m）	单向的 Hash 函数如,如有限域的幂运算
MAC（m）	由私钥 K 生成的消息认证，如 HMAC
A→B：m	A 传消息 m 给 B
K(c,k) ：	使用私钥 k 加密内容 c,如 Triple DES、RSA 算法，
D(c,k)	使用私钥 k 解密内容 c,如 Triple DES、RSA 算法，
igoods.content：	为信息商品的内容
igoods.id	为信息商品的标识
user_id	客户的标识的信息
Tag：	客户的环境的信息
A：	客户
B：	版权控制服务器
C：	内容服务器
Kb, Kb’	B 的公钥和私钥
Kplug ,Kplug' B	分配给插件的公钥和私钥

Protocol Content-Authentication Protocol

{

C: a=igoods_i.content //a 是商品 i 的内容

b=igoods_i.id //b 是商品 i 标识

kdes_i=nonce ,kmac_i=nonce //生成随机量 ki,kj

c= K(a,kdes_i) //使用 kdes_i 加密 a

d=HMAC(c,kmac_i) //使用 kmac_i 认证完整性

SecurityData = {b,kdes_i,kmac_i} //给版权控制的保密数据

Container = {b,c,d} //给用户的加密内容

C → A: Container ;

A: if Verify Container's integrity //验证内容容器的完整性

C →B: SecurityData

}

Protocol License Protocol (A,B)

{

A: infor1={ H(Tag),user_id}; //产生个人机器参数,用户标识

ask_mac= {Container.b,info1}

//内容的标识和用户的个人信息

A → B:en_ask_mac=K(ask_mac,kb)

//用版权控制服务程序的公钥加密 ask_mac

B : ask_mac=D(en_ask_mac,kb')

//用版权服务器的私钥解密。得到 ask_mac

Search SecutityData(ask_mac.Container.b)

//使用找到商品 i 保密数据

ret_data={kdes_i,kmac_i}

//将来给出商品 i 的解密密钥和认证密钥

en_ret_data=K(ret_data,ask_mac.infor1)

//使用用户信息加密商品 i 的解密密钥

```
B → A:   en_ret_data
A:   Save en_ret_data
                    //A 的插件程序保存收到的数据
A:              //循环使用商品 i
      infor2=i{ H(Tag),user_id}
//再次产生用户的机器参数，合法用户信息一定和 infor1 相同
      ret_data2=D(en_ret_data,infor2)
      if   Verify Container.d   integrity success
            //如果商品 i 可以由 kmac_i 认证完整性
      then
      {     igoods_i.context=D(Container.d,ret_data2.kdes_i)
            //解密内容数据
        Play igoods_i,context;                    //播放商品 i 的内容
      }
      else   Refuse
}
```

下面再参照图 8A-图 8D 的流程图对上述代码表示的协议进行详细说明。

图 8A 是内容服务器 C 形成内容容器的过程。目的是将要保护的数字媒体内容（文本，音乐等）通过加密形成内容容器 DPG，使得 DPG 的内容只能是通过得到密钥之后解密播放。同时对于内容容器添加消息文摘，通过消息文摘判断内容的完整性。

在图 8A 中，依次执行如下步骤：步骤 S1，由内容服务器 C 生成随机量 K1，K2 作为密钥；步骤 S2，用随机量 K1 加密信息商品内容形成 CPG；步骤 S3，使用 K2 认证 CPG 的完整性，使用 HMAC 形成加密的消息文摘 d = HMAC（CPG，K2）；步骤 S4，由信息商品的标识符 b，加密的内容 CPG，以及消息文摘 d 组合成内容容器 DPG；步骤 S5，将对应的信息商品的标识符及其对应的密钥 K1，K2 送给版权服务器 B。

图 8B 是客户认证内容容器的过程。目的是在客户得到加密的内容

容器之后，可以验证内容容器的完整性，验证不成功，不能打开加密的内容容器。

在图 8B 中，接着图 8A 的步骤 S5 执行如下步骤：步骤 S6，用户得到内容容器 DPG；步骤 S7，用户验证内容容器的完整性；步骤 S8，判断是否验证成功；如果在步骤 S8 中的判断为“否”，则转到步骤 S9 报告错误；如果在步骤 S8 中的判断为“是”，则转到步骤 S10 确认内容可以执行。

图 8C 是许可证的生成与传送过程。目的是为了解密特定的内容容器，同时能够按照客户方的版权的权利请求执行，需要从版权服务器取得对于特定的内容容器所需要的许可证，许可证通过专门的步骤生成，然后将许可证从版权服务器传送到客户方。

在图 8C 中，接着图 8B 的步骤 S10 执行如下步骤：步骤 S11，客户 A 取得个人的机器参数及其用户帐户形成 PInfo；步骤 S12，客户 A 组合信息商品内容 ID，特征 ID（表示权利要求）以及用户的 Pinfo，形成 LPG1；步骤 S13，客户 A 用版权服务器 B 的公钥加密 LPG1 得到 LPG2；步骤 S14，客户 A 将 LPG2 送给版权服务器 B；步骤 S15，版权服务器 B 用其私钥解开 LPG2，得到 LPG1；步骤 S16，在版权服务器 B 上搜索找到对应加密的内容容器的许可证；步骤 S17，返回生成的许可证；步骤 S18，使用用户个人信息加密许可证形成 LPG3；步骤 S19，版权服务器用 SSL 安全传送 LPG3 到用户（用户的插件程序完成用户的功能）。

图 8D 是客户在可信环境之中使用内容过程。目的是用户对于需要版权保护的内容在客户方的可信环境之中执行处理，其中内容和内容的密钥不会被泄露，而内容的显示、打印和编辑只是根据权利请求而执行。确保了内容不能被复制而且只是按照版权申请的权利要求执行。这是通过在 Web 浏览器的插件之中实现这一点。

在图 8D 中，接着图 8C 的步骤 S19 执行如下步骤：步骤 S20，客户 A 开始使用内容容器时，再次得到用户的机器参数 NInfo；步骤 S21，客户 A 用新产生的机器参数 Ninfo 作为密钥异或解开许可证；在步骤 S22 判断内容容器是否完整；如果在步骤 S22 中的判断结果为“否”则在步骤 S23 拒绝其内容并结束；如果在步骤 S22 中的判断结果为“是”，则

在步骤 S24 利用许可证密钥解密内容容器的数据；在步骤 S24 之后接着步骤 S25 播放或显示内容容器之中的内容，结束该协议过程。

5．系统安全性分析

系统的安全性的分析包括对于控制信息的安全通信、插件程序的隔离性两个方面的分析。首先是控制信息应该是安全传送：插件程序给版权服务器的信息是使用版权服务器的公钥来加密的，除开版权服务器没有人能解开控制信息；版权服务器发送给客户的信息使用了客户环境的个人机器参数加密，这样只有插件程序再次搜集客户的用户机器参数才能解开版权服务器的控制信息。其次，用户的消费是保密：用户发的客户环境信息是加扰后的。对于插件的隔离性是通过分析插件的信息流来判断的。插件只从浏览器接受数据和调用浏览器的功能发送数据，它不会直接联系客户的其他任务，它是被浏览起隔离的。攻击者必须先攻击浏览器，才能攻击插件。同时插件使用定时自动更新(定时下载取得新的密钥对)，加强自己的完整性保护。

6．系统实现与相关工作的比较

我们提出了一种实用的基于 Netscape Plugin(插件)的内容版权保护的计算机制 SKCC。现在我们已经实现了系统的部分功能。进一步的系统实现正在进行之中。我们选用的开发平台服务器方是 WindowsNT5.0，采用了 Apache Web Server1.3(for Windows)。客户方采用了 Windows98 系统，以及 Internet Explorer5.0, 以及利用 PluginSDK4.0。我们采用了独自实现的 RSA, DES,以 SHA, HMAC 算法的函数库。用 RSA 算法处理反对称密钥加密。采用 MD5 作为单向 Hash 函数。DES 作为对称的密钥加密。

说 明 书 附 图

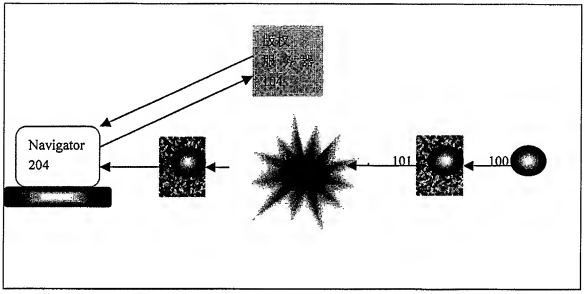


图 1

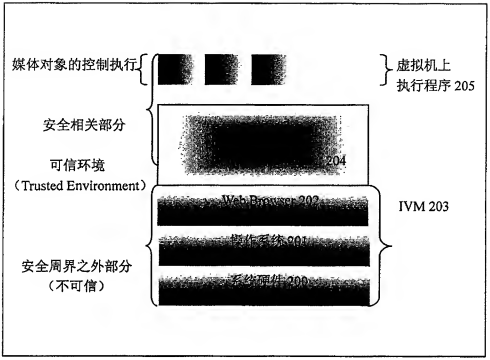

媒体对象的控制执行
虚拟机上
执行程序 205
安全相关部分
可信环境
（Trusted Environment）
204
IVM 203
安全周界之外部分
（不可信）

图 2

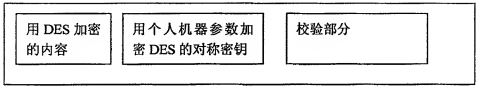

用 DES 加密的内容
用个人机器参数加密 DES 的对称密钥
校验部分

图 3A

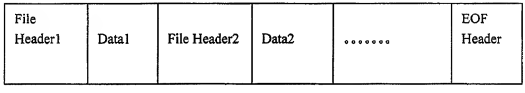

File Header1
Data1
File Header2
Data2
.....
EOF Header

图 3B

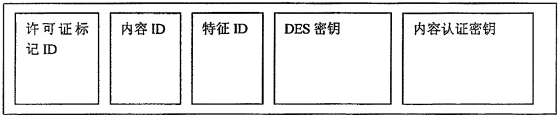

许可证标记 ID
内容 ID
特征 ID
DES 密钥
内容认证密钥

图 3C

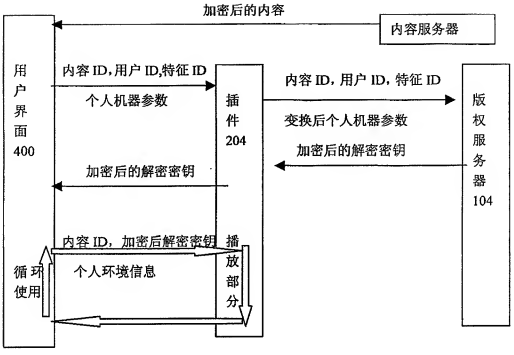

加密后的内容
内容服务器
用户界面400
内容ID，用户ID,特征ID
个人机器参数
插件204
内容ID，用户ID，特征ID
变换后个人机器参数
加密后的解密密钥
版权服务器104
加密后的解密密钥
内容ID，加密后解密密钥
个人环境信息
循环使用
播放部分

图 4

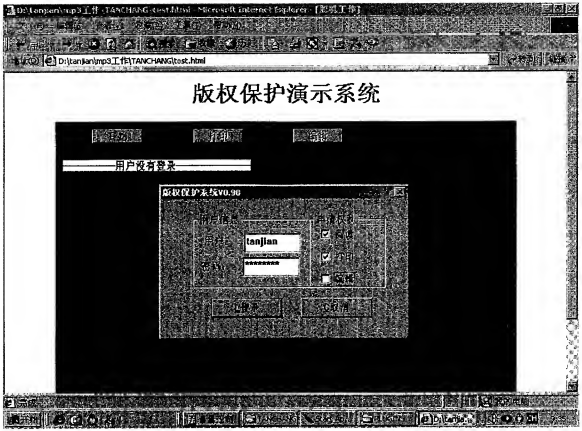


图 5

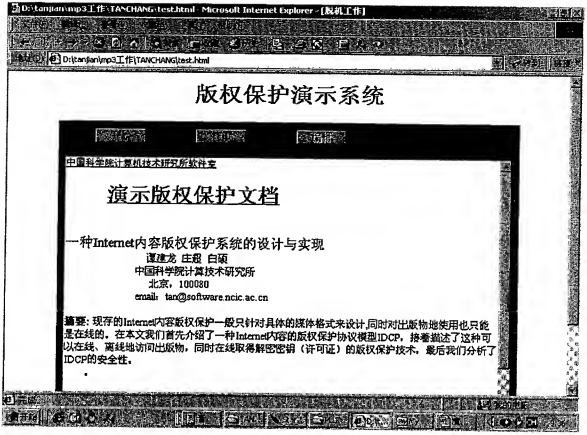

D:\tanjian\mp3工作\TANCHANG\test.html - Microsoft Internet Explorer - [脱机工作]
D:\tanjian\mp3工作\TANCHANG\test.html
版权保护演示系统
中国科学院计算机技术研究所软件室
演示版权保护文档
一种Internet内容版权保护系统的设计与实现
谭建龙 庄毅 白硕
中国科学院计算技术研究所
北京，100080
email：tan@software.ncic.ac.cn
摘要：现存的Internet内容版权保护一般只针对具体的媒体格式来设计，同时对出版物地使用也只能是在线的。在本文我们首先介绍了一种Internet内容的版权保护协议模型IDCP，接着描述了这种可以在线、离线地访问出版物，同时在线取得解密密钥（许可证）的版权保护技术。最后我们分析了IDCP的安全性。

图 6

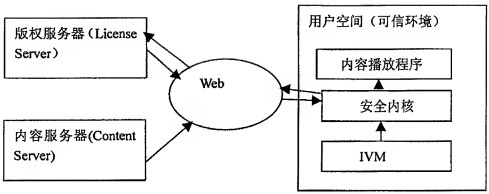

版权服务器（License Server）
内容服务器(Content Server)
Web
用户空间（可信环境）
内容播放程序
安全内核
IVM

图 7

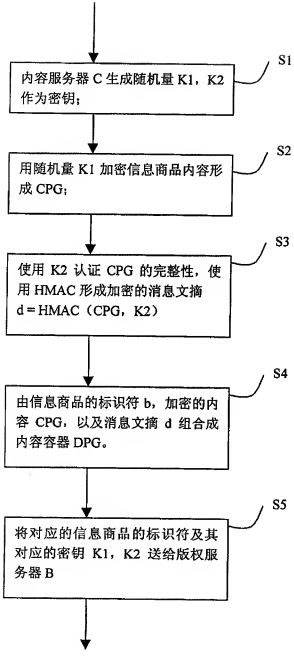

S1
内容服务器 C 生成随机量 K1，K2 作为密钥；
S2
用随机量 K1 加密信息商品内容形成 CPG；
S3
使用 K2 认证 CPG 的完整性，使用 HMAC 形成加密的消息文摘 d＝HMAC（CPG，K2）
S4
由信息商品的标识符 b，加密的内容 CPG，以及消息文摘 d 组合成内容容器 DPG。
S5
将对应的信息商品的标识符及其对应的密钥 K1，K2 送给版权服务器 B

图 8A

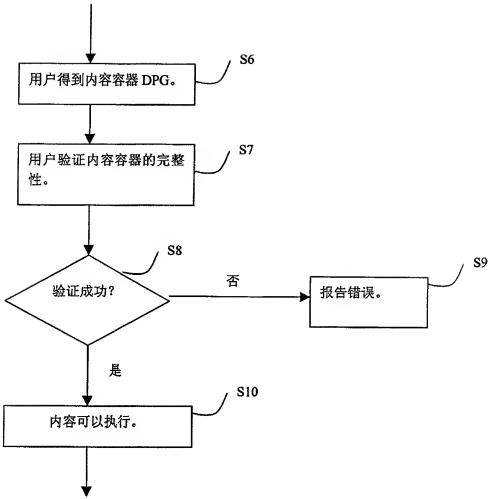

用户得到内容容器 DPG。
S6
用户验证内容容器的完整性。
S7
验证成功?
S8
否
报告错误。
S9
是
内容可以执行。
S10

图 8B

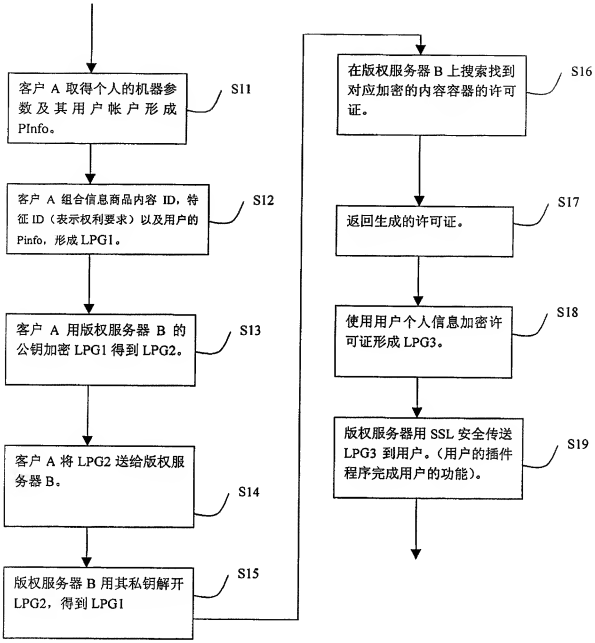

客户 A 取得个人的机器参数及其用户帐户形成 PInfo。
S11
客户 A 组合信息商品内容 ID，特征 ID（表示权利要求）以及用户的 Pinfo，形成 LPG1。
S12
客户 A 用版权服务器 B 的公钥加密 LPG1 得到 LPG2。
S13
客户 A 将 LPG2 送给版权服务器 B。
S14
版权服务器 B 用其私钥解开 LPG2，得到 LPG1
S15
在版权服务器 B 上搜索找到对应加密的内容容器的许可证。
S16
返回生成的许可证。
S17
使用用户个人信息加密许可证形成 LPG3。
S18
版权服务器用 SSL 安全传送 LPG3 到用户。（用户的插件程序完成用户的功能）。
S19

图 8C

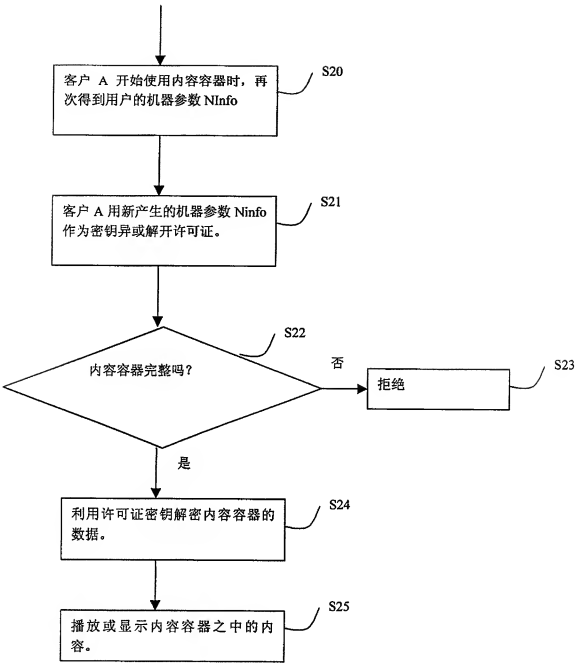

客户 A 开始使用内容容器时，再次得到用户的机器参数 NInfo
S20
客户 A 用新产生的机器参数 Ninfo 作为密钥异或解开许可证。
S21
内容容器完整吗？
S22
否
拒绝
S23
是
利用许可证密钥解密内容容器的数据。
S24
播放或显示内容容器之中的内容。
S25

图 8D

Copyright protecting method based on network browser card

Publication number: CN1361481

Publication date: 2002-07-31

Inventor: ZHUANG CHAO (CN); LI GUOJIE (CN); TAN JIANLONG (CN)

Applicant: INST OF COMPUTING TECH ACADEMI (CN)

Classification:

- international: ***G06F12/14; G06F12/16;*** **G06F12/14; G06F12/16;** (IPC1-7): G06F12/14; G06F12/16

- European:

Application number: CN20001036751 20001228

Priority number(s): CN20001036751 20001228

Abstract of **CN1361481**

The digital copyright protecting method controls the right of printing, editing and broadcasting digital published matter content via enciphering digital media content and license in network environment and including deciphering key. It includes the following steps: forming content container in content server; client confirmation of content container; license generation and transmission; and use of the content by the client in credible environment.